BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

HEDIN HALL LLP
David W. Hall (State Bar No. 274921)
Four Embarcadero Center, Suite 1400
San Francisco, CA 94111
Telephone: (415) 766-3534
Facsimile: (415) 402-0058
Email: dhall@hedinhall.com

Counsel for Plaintiff and the Putative Class

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MARIO CALDERON, individually and on behalf of all others similarly situated, Plaintiff, v. GOOGLE, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

On behalf of himself and all others similarly situated, Mario Calderon ("Plaintiff) brings this Class Action Complaint against Google LLC ("Google") for violation of Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, and alleges as follows based on personal knowledge as to himself, on the investigation of his counsel and the advice and consultation of certain third-party agents as to technical matters, and on information and belief as to other matters, and demands trial by jury.

NATURE OF ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Google in collecting, storing, and using his and other similarly situated individuals' biometric identifiers[1] and biometric information[2] (referred to collectively as "biometrics") without informed written consent, in direct violation of the BIPA.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics – particularly in the City of Chicago, which was recently selected by major national corporations as a "pilot testing site[] for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias" (740 ILCS 14/5(b)) – the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that a private entity like Google may not obtain and/or possess an individual's biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored, *see id.*; (2) informs

---

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and "face geometry," among others.

[2] "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier used to identify an individual.

that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored, and used, *see id.*; (3) receives a written release from the person for the collection of her biometric identifiers or information, *see id.*; and (4) publishes publically available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information, 740 ILCS 14/15(a).

4. In direct violation of each of the foregoing provisions of § 15(a) and § 15(b) of the BIPA, Google is actively collecting, storing, and using – without providing notice, obtaining informed written consent, or publishing data retention policies – the biometrics of all individuals who appear in photographs uploaded to Google Photos in Illinois.

5. Specifically, Google has created, collected, and stored, in conjunction with its cloud-based "Google Photos" service, the "face templates" (or "face prints") – highly detailed geometric maps of the face – of millions of users of the Google Photos service and hundreds of thousands of individuals who are not even enrolled in the Google Photos service. Google creates these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces that appear in photos taken on Google "Droid" devices and uploaded to the cloud-based Google Photos service. Each face template that Google extracts is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person.

6. Plaintiff brings this action to stop Google from further violating his privacy rights and the privacy rights of other individuals appearing in photographs uploaded to Google Photos in Illinois, and to recover statutory damages for Google's unauthorized collection, storage, and use of his biometrics and the biometrics of all others similarly situated in violation of the BIPA.

PARTIES

7. Plaintiff Calderon is, and has been at all relevant times, a resident and citizen of Chicago, Illinois. Plaintiff Calderon is an owner and user of a Google Android device and is an account holder and user of the Google Photos service.

8. Google is a Delaware corporation with its headquarters at 1600 Amphitheatre Parkway, Mountain View, California 94043. Accordingly, Google is a citizen of the states of

Delaware and California. Google is also registered to do business in Illinois (No. 65161605) and maintains an office in Cook County, Illinois.

JURISDICTION AND VENUE

9. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA"), because: (i) the proposed class consists of millions of members; (ii) the parties are minimally diverse with respect the proposed class because the members of the class, including Plaintiff, are citizens of a state different from Google's home states; and (iii) the aggregate amount in controversy with respect to the proposed class exceeds $5,000,000.00, exclusive of interests and costs. There are millions of individuals who use Google Photos and whose faces appeared in photographs uploaded to Google Photos from within Illinois, which Google used to extract scans of their facial geometry, and create and collect their face templates and face models, while they were residing in Illinois. The estimated number of individuals who were impacted by Google's conduct in Illinois multiplied by the BIPA's statutory liquidated damages figure ($5,000.00 for each intentional or reckless violation and $1,000.00 for each negligent violation) easily exceeds CAFA's $5,000,000.00 threshold, for each of the proposed classes.

10. Personal jurisdiction and venue are proper in California and within this District because Defendant maintains its corporate headquarters and principal place of business within this District, in Mountain View, California.

FACTUAL BACKGROUND

I. Biometric Technology Implicates Consumer Privacy Concerns

11. "Biometrics" refers to unique physical characteristics used to identify an individual. One of the most prevalent uses of biometrics is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific "biometric identifiers" (*i.e.*, details about the face's geometry as determined by facial points and contours), and comparing the resulting "face template" (or "faceprint") against the face templates stored in a "face template database." If a database match is found, an individual can be identified.

12. The use of facial recognition technology in the commercial context presents numerous consumer privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and carefully consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[3] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[4]

13. The Federal Trade Commission ("FTC") has raised similar concerns, and recently released a "Best Practices" guide for companies using facial recognition technology.[5] In the guide, the Commission underscores the importance of companies' obtaining affirmative consent from consumers before extracting and collecting their biometric identifiers and biometric information from digital photographs.

14. As explained below, Google failed to obtain consent from anyone when it introduced its facial recognition technology. Not only do the actions of Google fly in the face of FTC guidelines, they also violate the right to privacy conferred by the BIPA.

II. Illinois's Biometric Information Privacy Act

15. In 2008, Illinois enacted the BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. The BIPA makes it unlawful for a company to*, inter alia*, "collect,

---

[3] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012), *available at* https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf (last visited Feb. 18, 2020).

[4] *Id.*

[5] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (last visited Feb. 18, 2020).

capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers[6] or biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

740 ILCS 14/15 (b).

16. Section 15(a) of the BIPA also provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

17. As alleged below, Google's practices of collecting, storing and using biometric identifiers and information from photographs in Illinois without the requisite informed written consent violate all three prongs of § 15(b) of the BIPA. Google's failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of individuals' biometrics also violates § 15(a) of the BIPA.

III. Google Violates Illinois's Biometric Information Privacy Act

18. In 2011, Google's then-CEO Eric Schmidt discussed the company's past development of facial recognition technology, and explained that he had put the brakes on the

---

[6] BIPA's definition of "biometric identifier" expressly includes information collected about the geometry of the face (i.e., facial data obtained through facial recognition technology). *See* 740 ILCS 14/10.

program due to the profound implications he believed the technology would have on individuals' privacy rights. Characterizing facial recognition technology as "crossing the creepy line," Mr. Schmidt said at the time "that [Google] would not build a database capable of recognizing individual faces even though it is increasingly possible." Warman, Matt, "Google warns against facial recognition database," The Telegraph, May 18, 2011, *available at* http://www.telegraph.co.uk/technology/google/8522574/Google-warns-against-facial-recognition-technology.html. Nonetheless, Mr. Schmidt predicted that "some company by the way is going to cross that line." *Id.*

19. In 2013, Mr. Schmidt wrote a piece for The Wall Street Journal, titled "The Dark Side of the Digital Revolution," in which he again cautioned against the collection of Americans' biometric data and advocated in favor of regulating the collection and use of such data in this country, writing in pertinent part:

> Today's facial-recognition systems use a camera to zoom in on an individual's eyes, mouth and nose, and extract a "feature vector," a set of numbers that describes key aspects of the image, such as the precise distance between the eyes. (Remember, in the end, digital images are just numbers.) Those numbers can be fed back into a large database of faces in search of a match. The accuracy of this software is limited today (by, among other things, pictures shot in profile), but the progress in this field is remarkable. A team at Carnegie Mellon demonstrated in a 2011 study that the combination of "off-the-shelf" facial recognition software and publicly available online data (such as social network profiles) can match a large number of faces very quickly. With cloud computing, it takes just seconds to compare millions of faces. The accuracy improves with people who have many pictures of themselves available online—which, in the age of Facebook, is practically everyone.
>
> By indexing our biometric signatures, some governments will try to track our every move and word, both physically and digitally. That's why we need to fight hard not just for our own privacy and security, but also for those who are not equipped to do so themselves. We can regulate biometric data at home in democratic countries, which helps.

Schmidt, Eric, "The Dark Side of the Digital Revolution," The Wall Street Journal, Apr. 19, 2013, *available at* https://www.wsj.com/articles/SB10001424127887324030704578424650479285218.

20. Ironically, the company that Google's CEO predicted in 2011 would one day "cross that line" by diving into the consumer facial recognition turned out to be Google itself.

21. In May 2015, Google announced the release of its web- and mobile app-based photo sharing and storage service called Google Photos. Users of Google Photos immediately began uploading millions of photos per day through the service, and Google in turn began using its "FaceNet"-powered facial recognition technology to extract, collect, store, and catalog the biometric data of everyone whose faces appeared in all of those uploaded photographs, in real time.[7]

22. The Google Photos service uses web- and app-based APIs developed and maintained by Google that are powered by Google's proprietary "FaceNet" architecture. Increasingly, Google has licensed its Google Photos APIs, including APIs that enable the use of its facial recognition technology, to mobile application developers who develop consumer-facing mobile applications for use in various contexts. Google sells licenses to its APIs to these third parties for money, and derives substantial commercial profit from such sales. Thus, less than four years after warning of the immense dangers posed by facial recognition technology, Google unleashed that very technology on the world's citizens in pursuit of greater corporate profits.

23. The Google Photos app, which comes pre-installed on all Google Android devices, is set by default to automatically upload all photos taken by the Droid device user to the cloud-based Google Photos service. Users can also connect other devices to Google Photos to upload to and access photos on the cloud-based service.

24. Unbeknownst to the average consumer, and in direct violation of § 15(b)(1) of the BIPA, Google's proprietary facial recognition technology scans each and every photo uploaded to the cloud-based Google Photos service for faces, extracts geometric data relating to the unique

---

[7] A research paper released by Google engineers at around the same time as the release of Google Photos describes FaceNet as "a unified system for face verification (is this the same person), recognition (who is this person) and clustering (find common people among these faces)." Schroff, Florian, et al., "FaceNet: A Unified Embedding for Face Recognition and Clustering," June 7, 2015, available at https://ieeexplore.ieee.org/document/7298682.

points and contours (i.e., biometric identifiers) of each face, and then uses that data to create and store a template of each face – all without ever informing anyone of this practice.[8]

25. These unique face templates are not only collected and used by Google to identify individuals by name, but also to recognize their gender, age, and location. Accordingly, Google also collects "biometric information" from individuals appearing in photographs uploaded to Google Photos. *See* 740 ILCS 14/10.

26. In direct violation of §§ 15(b)(2) and 15(b)(3) of the BIPA, Google never informed its users who had their face templates collected of the specific purpose and length of term for which their biometric identifiers or information would be collected, stored, and used, nor did Google obtain a written release from any of these individuals.

27. In direct violation of § 15(a) of the BIPA, Google does not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying biometric identifiers or information.

28. The cloud-based Google Photos service uses these face templates to organize and group together photos based upon the particular individuals appearing in the photos. This technology works by comparing the face templates of individuals who appear in newly-uploaded photos with the facial templates already saved in Google's face database. Specifically, when a Google Photos user uploads a new photo, Google's sophisticated facial recognition technology creates a template for each face depicted therein, and then compares each template against Google's database of face templates. If there is a match, then Google groups the photo from which the newly-uploaded face template was derived with the previously uploaded photos depicting that individual, and further refines its accuracy by storing and grouping the corresponding face template with other previously collected and stored templates pertaining to the same person's face, in order to generate a more sophisticated, uniquely identifying "face model" corresponding to each person's facial geometry.

---

[8] Google holds several patents covering its facial recognition technology that detail its illegal process of scanning photos for biometric identifiers and storing face templates in its database without obtaining informed written consent.

29. Google also uses its FaceNet-powered facial recognition technology to power the facial recognition capabilities of its Nest Cam, a consumer home-security product that is able to recognize and identify individuals whose faces are detected in the video feed of the camera. To comply with BIPA in Illinois, Google has chosen not to apply its facial recognition technology to the faces of individuals who appear on its Nest Cams in the state of Illinois; Google refrains from scanning the facial geometry of people who appear on its Nest Cams in Illinois by using the IP addresses and other geolocation identifiers associated with its Nest Cams to disable its facial recognition technology on those devices being operated within the state of Illinois's boundaries.

30. Google could have refrained from applying its facial recognition technology to photographs uploaded to Google Photos in Illinois in the same way that it refrained from applying its facial recognition technology to the video feeds generated by its Nest Cams in Illinois. Indeed, as long ago as late 2017, Google was able to program its facial recognition technology to refrain from collecting scans of facial geometry, or from creating face templates, from photographs uploaded to Google's "Webb" mobile application (which compares faces to historical paintings) from within Illinois and Texas, in order to comply with BIPA and a similar Texas law that governs companies' collection and storage of biometrics. By using the IP addresses and other geolocation identifiers associated with the devices on which the "Webb" app is installed, Google was able to refrain from applying its facial recognition technology to photographs uploaded from devices using the application in Illinois and Texas. Despite possessing the technological wherewithal to bring Google Photos in compliance with BIPA in Illinois, in the same way it did with "Webb," Google has chosen not to make Google Photos compliant with BIPA. Over the past five years, Google has instead chosen to systematically create and store face templates, *en masse,* for every person (including everyone in Illinois) whose face appears in a photograph uploaded to Google Photos, without asking for much less obtaining the requisite prior informed written consent to engage in these practices.

31. Moreover, Google has also limited its collection of scans of face geometry to photographs uploaded from certain countries (beginning with the United States, with gradual expansion elsewhere) by using IP addresses to determine the geographical locations of incoming

photographs. *See* James Vincent, "Facebook's New Photo App Won't Launch In Europe Because of Facial Recognition," The Verge, http://www.theverge.com/2015/6/19/8811617/facebook-moments-facial-recognition-europe (June 19, 2015) ("Google's recently-launched Google Photos app — which uses facial recognition to sort snaps by who's in them — also limits its use of the technology to the US."); Google LLC, "Updates & Announcements for Oct. 28, 2015, Google Photos," https://plus.google.com/+GooglePhotos/posts/EPjgwrsrRyF ("Rolling out on all platforms, here's what's new: … Face grouping will be available in Latin America, Canada, the Caribbean, Australia, and New Zealand. It will also be available in parts of Asia, the Middle East, and Africa."); Jason Bouwmeester, "HOW TO; Enable the 'Group Similar Faces' People Function in Google Photos," Techaeris, http://techaeris.com/2015/05/31/how-to-enable-the-group-similar-faces-people-function-in-google-photos/ (May 31, 2015) (explaining that Google Photos facial recognition technology is only available on devices that have "a U.S. IP address").

32. In sum, BIPA clearly prohibits what Google has done, Google has been fully aware of that since the day it launched Google Photos, and Google has made no efforts to come into compliance with BIPA at any time in the five years since (be it by obtaining the requisite signed written release from its users in Illinois or turning the technology off in Illinois altogether).

IV. Plaintiff Calderon's Experience

33. During the time period relevant to this action, Plaintiff Calderon purchased a Google Android device from a retail location in Illinois and, using that device, enrolled his pre-existing Google account in the Google Photos service, which then became automatically linked to his Android device.

34. Since purchasing his Google Android device up until the present, Plaintiff Calderon has at all times resided in Illinois. While residing in Illinois, Plaintiff Calderon has used his Google Android device to take hundreds of photos of himself, depicting his face, in the state of Illinois. Upon taking these photos, his Android device automatically uploaded the photos to his cloud-based Google Photos account. These photos were all uploaded to the cloud-based Google Photos service while the Google Android device was located in the state of Illinois and assigned an Illinois-based IP address.

35. Immediately upon upload to the cloud-based Google Photos storage service, Google analyzed these photos, automatically located and scanned Plaintiff Calderon's face, extracted geometric data relating to the contours of his face and the distances between his eyes, nose, and ears, and then used that data pertaining to his facial geometry to create a unique template of his face.

36. The resulting "face templates" created by Google were unique to Plaintiff Calderon.

37. Plaintiff Calderon's face template was also used by Google to recognize Plaintiff Calderon's gender, age, race, and location.

38. Google therafter compiled its collection of the various "face templates" that it had created from the facial geometry it had extracted from the various photographs of Plaintiff Calderon's face in order to create and store an even more sophisticated and detailed "face model" of Plaintiff Calderon's facial geometry. As with the "face models" that Google created and stored for all other members of the proposed Class, the "face model" that Google created and stored for Plaintiff Calderon is associated with Plaintiff Calderon's name and his Google Photos account, uniquely identifies Plaintiff Calderon by his face in the same way that a fingerprint identifies one and only one person, and is used by Google to locate and group together all photos depicting Plaintiff Calderon for organizational purposes.

39. Neither Plaintiff Calderon nor any member of the proposed Class received a disclosure from Google that it would collect, capture, otherwise obtain, or store their unique biometric identifiers or biometric information from photographs, and neither Plaintiff Calderon nor any member of the proposed Class ever consented, agreed or gave permission – via a written release or otherwise – to authorize or permit Google to collect, capture, otherwise obtain, or store their unique biometric identifiers or biometric information in this way.

40. Likewise, Google never provided Plaintiff Calderon or any other member of the Class with an opportunity to prohibit or prevent the collection, storage, or use of their unique biometric identifiers or biometric information.

41. Nevertheless, when photos of Plaintiff Calderon and the unnamed members of the Class were automatically uploaded to Google Photos from within the state of Illinois, Google

located Plaintiff Calderon's and the unnamed Class members' faces in the photos, scanned each of their facial geometry, and created unique "face templates" and even more detailed "face models" corresponding to Plaintiff Calderon and each member of the proposed Class, all in direct violation of the BIPA.

CLASS ALLEGATIONS

42. **Proposed Class Definition:** Plaintiff Calderon brings this action pursuant to Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All Google Photos users located in Illinois for whom Google created and stored a face template after May 28, 2015.

43. **Numerosity:** The number of persons within the Class is substantial, believed to amount to millions of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation.

44. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from member to member of each respective Class, and which may be determined without reference to the individual circumstances of any member of either Class, include but are not limited to the following:

a) whether Google collected, captured, or otherwise obtained Plaintiff's and the Class's "biometric identifiers" or "biometric information";

b) whether Google stored Plaintiff's and the Class's "biometric identifiers" or "biometric information";

c) whether Google properly informed Plaintiff and the Class that it would collect,

capture, otherwise obtain and then store their "biometric identifiers" or "biometric information";

d) whether Google obtained a written release (as defined in 740 ILCS 14/10) prior to collecting, capturing, or otherwise obtaining, and then storing, Plaintiff's and the Class's "biometric identifiers" or "biometric information";

e) whether Google developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying "biometric identifiers" and "biometric information" when the initial purpose for collecting, capturing, or otherwise obtaining these "biometric identifiers" and "biometric information" has been satisfied or within 3 years of their last interaction with Plaintiff and members of the Class, whichever occurs first;

f) whether Google used Plaintiff's and the Class's "biometric information" to identify them;

g) whether Google's violations of the BIPA were committed negligently; and

h) whether Google's violations of the BIPA were committed intentionally or recklessly;

45. **Adequate Representation:** Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Neither Plaintiff, nor any of his counsel, have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

46. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members

of the Class is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with the BIPA.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/1, et seq.
(On Behalf of Plaintiff and the Class)

47. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

48. The BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

49. Google is a corporation and thus qualifies as a "private entity" under the BIPA. *See* 740 ILCS 14/10.

50. Plaintiff and the Class members are Google Photos users located in Illinois who had their "biometric identifiers," including scans of face geometry, collected, captured, received, or otherwise obtained by Google from photographs that were uploaded to Google Photos after May 28, 2015, which Google used to create and store millions of "face templates" that uniquely identify Plaintiff and each member of the Class. *See* 740 ILCS 14/10.

51. Plaintiff and the Class members are individuals who had their "biometric information" collected by Google (in the form of their gender, age, and location) through Google's collection and use of information derived from their "biometric identifiers" that is used to identify them.

52. Google systematically and automatically collected, captured, or otherwise obtained Plaintiff Calderon's and the Class members' "biometric identifiers" (which it used to create and store their uniquely identifying "face templates") and "biometric information" without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them.

53. In fact, Google failed to properly inform Plaintiff or the Class in writing that their "biometric identifiers" and "biometric information" were being "collected or stored" on Google Photos, nor did Google inform Plaintiff or the Class members in writing of the specific purpose and length of term for which their "biometric identifiers" and "biometric information" were being "collected, stored and used" as required by 740 ILCS 14/15(b)(1)-(2).

54. In addition, Google does not publicly provide a retention schedule or guidelines for permanently destroying the "biometric identifiers" and "biometric information" of Plaintiff or the Class members, as required by the BIPA. *See* 740 ILCS 14/15(a).

55. By collecting, storing, and using Plaintiff's and the Class's "biometric identifiers" and "biometric information" as described herein, Google recklessly or intentionally violated each of BIPA's requirements, and infringed the rights of Plaintiff and each Class member to keep private this sensitive, immutable, and uniquely identifying biometric data.

56. On behalf of himself and the proposed Class members, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Google to comply with the BIPA's requirements for the collection, capture, and storage of "biometric identifiers" and "biometric information" as described herein; (2) statutory damages of $1,000.00 pursuant to 740 ILCS 14/20 for each negligent violation of BIPA committed by Google; (3) statutory damages of $5,000.00 pursuant to 740 ILCS 14/20 for each intentional or reckless violation of BIPA committed by Google; and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing his counsel as Class Counsel of the Class;

B. Declaring that Google's actions, as set out above, violate the BIPA, 740 ILCS l4/1, *et seq.*, with respect to Plaintiff and members of the Class;

C. Awarding statutory damages to Plaintiff and the Class members of $1,000.00 pursuant to 740 ILCS 14/20(1) for each violation of BIPA committed negligently, and $5,000.00 pursuant to 740 ILCS 14/20(2) for each violation of BIPA committed intentionally or recklessly;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and members of the Class, including, *inter alia*, an order requiring Google to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees pursuant to BIPA;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable;

G. Awarding Plaintiff and the Class such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

On behalf of himself and all others similarly situated, Plaintiff demands a trial by jury pursuant to Federal Rule of Civil Procedure 38(b) on all claims and issues so triable

Dated: February 19, 2020

BURSOR & FISHER, P.A.

By: */s/ L. Timothy Fisher*

L. Timothy Fisher (State Bar No. 191626)

1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Scott A. Bursor (State Bar No. 276006)
2665 S. Bayshore Dr., Suite 220
Miami, FL 33133
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: scott@bursor.com

HEDIN HALL LLP
David W. Hall (State Bar No. 274921)
Four Embarcadero Center, Suite 1400
San Francisco, CA 94111
Telephone: (415) 766-3534
Facsimile: (415) 402-0058
Email: dhall@hedinhall.com

HEDIN HALL LLP
Frank S. Hedin (State Bar No. 291289)
1395 Brickell Avenue, Suite 1140
Miami, Florida 33131
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
Email: fhedin@hedinhall.com

Counsel for Plaintiff and the Putative Class